SECTION OF HIPAA SECURITY RULE	HIPAA SAFEGUARD	RELEVANT FISMA PROVISIONS	RELEVANT DITSCAP PROVISIONS As stated in the P3WG[1] relevant to DoD 8510.1-M	DoD Relevant References
ADMINISTRATIVE SAFEGUARDS				
164.308(a)(1)(i)	**Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations.**	**Ref §3544(a)(b)(1)** "Periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency."	**NONE**	DoD 5160.54-D DoD 5200.40-I DoD 8500.1-D DoD 8500.2-I DoD 8000.1-D MHS IA Policy/Guidance Manual (Feb 2003)
164.308(a)(1)(ii)(A)	Risk Analysis: Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.	**Ref §3544(a)(b)(1)** "Periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency."	**PARTIAL** - Section C3.4.4.2.3.1 requires the CA team to "evaluate the degree of risk to the system. The cost benefit analysis of alternative is then used to identify appropriate cost-effective countermeasures to mitigate the risk. These countermeasures include technical, physical, personnel, and administrative countermeasures." The results of this requirement are documented in section 2.3 and appendix Q. However, "In Phase 2, the vulnerability assessment concentrates on the sufficiency of specified technical requirements to protect and secure the information resources." While the countermeasures chosen can come from all of the various security disciplines it appears that the vulnerabilities that they are meant to counter are technical ones only. The concentration on technical vulnerabilities without regard to organizational questions makes risk analysis in this phase a partial one only.	DoD 5160.54-D DoD 5200.40-I DoD 8500.1-D DoD 8500.2-I MHS IA Policy/Guidance Manual (Feb 2003)
164.308(a)(1)(ii)(B)	Risk Management (R): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a).	**Ref §3544(b)(2)** "policies and procedures that—(A) are based on the risk assessments required by paragraph (1);(B) cost-effectively reduce information security risks to an acceptable level; (C) ensure that information security is addressed throughout the life cycle of each agency information system; and (D) ensure compliance with—(i) the requirements of this subchapter; (ii) policies and procedures as may be prescribed by the Director, and information security standards promulgated under section 11331 of title 40; (iii) minimally acceptable system configuration requirements, as determined by the agency; and (iv) any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President...."	**MEETS** – Chapter 2 states the purpose of the DITSCAP is to protect and secure DoD entities through a standardized process that balances, benefit, risk, and cost. Section C2.2 inclusive of all subsections covers the use of a Risk management approach in the DITSCAP process. Section C3.4.4.2.3 requires the CA team to define and document in the SSAA "the potential threats and single points of failure that can affect the confidentiality, integrity, and availability of the system. Clearly state the nature of the threat that is expected and where possible, the expected frequency of occurrence." This documents the first part of the risk management process. Section C3.4.4.2.3.1 requires the CA team to "evaluate the degree of risk to the system. The cost benefit analysis of alternative is then used to identify appropriate cost-effective countermeasures to mitigate the risk." Evaluating the risk and identifying countermeasures is a portion of the first two parts of risk management. The results of this requirement are documented in section 2.3 and appendix Q. In section C6.2.1.2 as part of the task description for risk management in phase 4 it states that risk management is the…"ongoing process that manages risk against the IS, the computing environment, and its resources. Effective management of the risk continuously evaluates…" This implements the ongoing maintenance and revision process that is part of good risk management. Section C3.4.5.2.1 requires the CA team to identify and document "the security instructions or directives applicable to the system." The HIPAA security and privacy standards would be among the national level directives that would be identified as requirements to be met by health related systems and networks and thus incorporated into the DITSCAP process. It does/would not refer to HIPAA by name however.	DoD 5000.1-D DoD 5000.2-R DoD 5160.54-D DoD 5200.40-I DoD 8500.1-D DoD 8500.2-I DoD 8510.1-M MHS IA Policy/Guidance Manual (Feb 2003)

SECTION OF HIPAA SECURITY RULE	HIPAA SAFEGUARD	RELEVANT FISMA PROVISIONS	RELEVANT DITSCAP PROVISIONS As stated in the P3WG[1] relevant to DoD 8510.1-M	DoD Relevant References
164.308(a)(1)(ii)(C)	Sanction Policy: Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.		**PARTIAL** - Appendix M of the SSAA is to include the documented Personnel Controls. This manual does not specifically state the types of personnel controls required, just that all personnel controls should be documented in this appendix.	DoD 5000.2-R
164.308(a)(1)(ii)(D)	Information System Activity Review: Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.		**PARTIAL** - Appendix I of the SSAA is to contain Applicable System Development Artifacts or System Documentation. One of the system documents required for systems that must meet the C2 level of assurance (all DoD health systems must be at least C2) is a Trusted Facility Manual, which must contain all of the information needed by the ISSO/SA to review and maintain activity logs and audit trails. This meets the requirement for documentation of the information system activity review procedure under § 164.316, policies and procedures documentation.	DoD 8500.1-D DoD 8500.2-I MHS IA Policy/Guidance Manual (Feb 2003)
164.308(a)(2)	**Assigned Security Responsibility: Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.**	**Ref §3544(a)(3)** "delegate to the agency Chief Information Officer established under section 3506 (or comparable official in an agency not covered by such section) the authority to ensure compliance with the requirements imposed on the agency under this sub-chapter, including—''(A) designating a senior agency information security officer...."	**MEETS-**Section C8.4.1 states that the "DAA is the primary government official responsible for system security." Section C3.4.7.2 requires section 5 of the SSAA to document "the appropriate authorities." This meets the requirement to document who has the assigned security responsibility.	DoD 5200.40-I DoD 8000.1-D DoD 8500.1-D DoD 8500.2-I MHS IA Policy/Guidance Manual (Feb 2003)
164.308(a)(3)(i)	**Workforce Security: Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.**		**PARTIAL** - Appendix M of the SSAA is to include the documented Personnel Controls. This manual does not specifically state the types of personnel controls required, just that all personnel controls should be documented in this appendix.	DoD 5200.2-D DoD 5200.2-R DoD 8500.1-D DoD 8500.2-I MHS IA Policy/Guidance Manual (Feb 2003)
164.308(a)(3)(ii)(A)	Authorization and/or Supervision: Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.		**PARTIAL** - Appendix M of the SSAA is to include the documented Personnel Controls. This manual does not specifically state the types of personnel controls required, just that all personnel controls should be documented in this appendix.	DoD 8500.2-I

SECTION OF HIPAA SECURITY RULE	HIPAA SAFEGUARD	RELEVANT FISMA PROVISIONS	RELEVANT DITSCAP PROVISIONS As stated in the P3WG[1] relevant to DoD 8510.1-M	DoD Relevant References
164.308(a)(3)(ii)(B)	Workforce Clearance Procedure: Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.		**PARTIAL** - Appendix M of the SSAA is to include the documented Personnel Controls. This manual does not specifically state the types of personnel controls required, just that all personnel controls should be documented in this appendix.	DoD 5200.2-D DoD 5200.2-R DoD 8500.2-I MHS IA Policy/Guidance Manual (Feb 2003)
164.308(a)(3)(ii)(C)	Termination Procedure: Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.		**PARTIAL** - Appendix M of the SSAA is to include the documented Personnel Controls. This manual does not specifically state the types of personnel controls required, just that all personnel controls should be documented in this appendix.	DoD 8500.2-I MHS IA Policy/Guidance Manual (Feb 2003)
164.308(a)(4)(i)	**Information Access Management: Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.**	**Ref §3544(b)(2)** "policies and procedures that—(A) are based on the risk assessments required by paragraph (1);(B) cost-effectively reduce information security risks to an acceptable level; (C) ensure that information security is addressed throughout the life cycle of each agency information system; and (D) ensure compliance with—(i) the requirements of this subchapter; (ii) policies and procedures as may be prescribed by the Director, and information security standards promulgated under section 11331 of title 40; (iii) minimally acceptable system configuration requirements, as determined by the agency; and (iv) any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President...."	**PARTIAL** - Section C3.4.2.2.3.4 requires the SSAA to "define the user's security clearances, their access rights to specific categories of information processed, and the actual information that the system is required to process." This information is recorded in section 1.3.4 of the SSAA. Does not require that the written policies and procedures for granting those authorizations exist.	DoD 8500.1-D DoD 8500.2-I MHS IA Policy/Guidance Manual (Feb 2003)
164.308(a)(4)(ii)(A)	Isolating Health Care Clearinghouse Function: If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.		**NONE**	N/A

SECTION OF HIPAA SECURITY RULE	HIPAA SAFEGUARD	RELEVANT FISMA PROVISIONS	RELEVANT DITSCAP PROVISIONS As stated in the P3WG[1] relevant to DoD 8510.1-M	DoD Relevant References
164.308(a)(4)(ii)(B)	Access Authorization: Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.		**PARTIAL** - Section C3.4.2.2.3.4 requires the SSAA to "define the user's security clearances, their access rights to specific categories of information processed, and the actual information that the system is required to process." This information is recorded in section 1.3.4 of the SSAA. Does not require that the written policies and procedures for granting those authorizations exist.	DoD 8500.1-D DoD 8500.2-I MHS IA Policy/Guidance Manual (Feb 2003)
164.308(a)(4)(ii)(C)	Access Establishment and Modification: Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.		**NONE**	DoD 8500.2-I MHS IA Policy/Guidance Manual (Feb 2003)
164.308(a)(5)(i)	**Security Awareness and Training: Implement a security awareness and training program for all members of its workforce (including management).**	**Ref §3544(b)(4)** ''security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of—(A) information security risks associated with their activities; and (B) their responsibilities in complying with agency policies and procedures designed to reduce these risks...."	**MEETS** - Section C3.4.4.2.1.8 requires the SSAA to "identify the training for individuals associated with the system's operation and determine if the training is appropriate to their level and area of responsibility. This training should provide information about the security policy governing the information being processed as well as potential threats and the nature of the appropriate countermeasures." The Security Education, Training, and Awareness Plan is documented in Appendix O.	DoD 8500.1-D DoD 8500.2-I MHS IA Policy/Guidance Manual (Feb 2003)
164.308(a)(5)(ii)(A)	Security Reminders: Implement periodic security updates.		**NONE**	MHS IA Policy/Guidance Manual (Feb 2003)
164.308(a)(5)(ii)(B)	Protection from Malicious Software: Implement Procedures for guarding against, detecting, and reporting malicious software.		**NONE**	MHS IA Policy/Guidance Manual (Feb 2003)
164.308(a)(5)(ii)(C)	Log-in Monitoring: Implement procedures for monitoring log-in attempts and reporting discrepancies.		**NONE**	No Policy Available
164.308(a)(5)(ii)(D)	Password Management: Implement procedures for creating, changing, and safeguarding passwords.		**NONE**	MHS IA Policy/Guidance Manual (Feb 2003)

SECTION OF HIPAA SECURITY RULE	HIPAA SAFEGUARD	RELEVANT FISMA PROVISIONS	RELEVANT DITSCAP PROVISIONS As stated in the P3WG[1] relevant to DoD 8510.1-M	DoD Relevant References
164.308(a)(6)(i)	**Security Incident Procedures: Implement policies and procedures to address security incidents.**	**Ref §3544(b)(7)** ''procedures for detecting, reporting, and responding to security incidents, consistent with standards and guidelines issued pursuant to section 3546(b), including—(A) mitigating risks associated with such incidents before substantial damage is done; (B) notifying and consulting with the Federal information security incident center referred to in section 3546; and (C) notifying and consulting with, as appropriate—(i) law enforcement agencies and relevant Offices of Inspector General; (ii) an office designated by the President for any incident involving a national security system; and (iii) any other agency or office, in accordance with law or as directed by the President...."	**PARTIAL** - Appendix K of the SSAA is to contain the Incident Response Plan. This meets the requirement to document the security incident procedures as required under § 164.316, policies and procedures documentation.	DoD 5215.2-I DoD 8500.1-D DoD 8500.2-I MHS IA Policy/Guidance Manual (Feb 2003)
164.308(a)(6)(ii)	Response and Reporting: Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.	**Ref §3544(b)(7)** ''procedures for detecting, reporting, and responding to security incidents, consistent with standards and guidelines issued pursuant to section 3546(b), including—''(A) mitigating risks associated with such incidents before substantial damage is done; (B) notifying and consulting with the Federal information security incident center referred to in section 3546; and (C) notifying and consulting with, as appropriate—'(i) law enforcement agencies and relevant Offices of Inspector General;' (ii) an office designated by the President for any incident involving a national security system; and (iii) any other agency or office, in accordance with law or as directed by the President..."	**NONE**	DoD 5215.2-I DoD 8500.1-D DoD 8500.2-I MHS IA Policy/Guidance Manual (Feb 2003)

SECTION OF HIPAA SECURITY RULE	HIPAA SAFEGUARD	RELEVANT FISMA PROVISIONS	RELEVANT DITSCAP PROVISIONS As stated in the P3WG[1] relevant to DoD 8510.1-M	DoD Relevant References
164.308(a)(7)(i)	**Contingency Plan: Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.**	**Ref §3544(b)(8)** "...plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency."	**MEETS** - C5.3.8. States that task 3-7 is “Contingency Plan Evaluation.” The task description in subsection C5.3.8.2 states, “The contingency plan evaluation task analyzes the contingency, backup, and continuity of service plans to ensure the plans are consistent with the requirements identified in the SSAA. Periodic testing of the contingency plan is required by DoD Directive 5200.28 (reference (b)) for critical systems and is encouraged for all systems.” Documents that partially satisfy the requirement for Contingency Plan **PARTIAL** - Appendix L of the SSAA is to contain the Contingency Plans. This meets the requirement to document the plans as required under § 164.316, policies and procedures documentation.	DoD 5200.40-I DoD 8500.2-I MHS IA Policy/Guidance Manual (Feb 2003)
164.308(a)(7)(ii)(A)	Data Backup Plan: Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.		**MEETS** - C5.3.8. States that task 3-7 is “Contingency Plan Evaluation.” The task description in subsection C5.3.8.2 states, “The contingency plan evaluation task analyzes the contingency, backup, and continuity of service plans to ensure the plans are consistent with the requirements identified in the SSAA. Periodic testing of the contingency plan is required by DoD Directive 5200.28 (reference (b)) for critical systems and is encouraged for all systems.” Documents that partially satisfy the requirement for Data Backup Plan **PARTIAL** - Appendix L of the SSAA is to contain the Contingency Plans. A Data Backup Plan is normally part of a DoD Contingency Plan. This meets the requirement to document the plans as required under § 164.316, policies and procedures documentation.	DoD 5200.40-I DoD 8500.2-I MHS IA Policy/Guidance Manual (Feb 2003)
164.308(a)(7)(ii)(B)	Disaster Recovery Plan: Establish (and implement as needed) procedures to restore any loss of data.	**Ref §3544(b)(8)** "...plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency."	**PARTIAL** - Appendix L of the SSAA is to contain the Contingency Plans. A Disaster Recovery Plan is normally part of a DoD Contingency Plan. This meets the requirement to document the plans as required under § 164.316, policies and procedures documentation.	DoD 5200.40-I DoD 8500.2-I MHS IA Policy/Guidance Manual (Feb 2003)
164.308(a)(7)(ii)(C)	Emergency Mode Operation Plan: Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.	**Ref §3544(b)(8)** "...plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency."	**PARTIAL** - Appendix L of the SSAA is to contain the Contingency Plans. An Emergency Mode Operations Plan is normally part of a DoD Contingency Plan. This meets the requirement to document the plans as required under § 164.316, policies and procedures documentation.	DoD 5200.40-I DoD 8500.2-I MHS IA Policy/Guidance Manual (Feb 2003)

SECTION OF HIPAA SECURITY RULE	HIPAA SAFEGUARD	RELEVANT FISMA PROVISIONS	RELEVANT DITSCAP PROVISIONS As stated in the P3WG[1] relevant to DoD 8510.1-M	DoD Relevant References
164.308(a)(7)(ii)(D)	Testing and Revision Procedure: Implement procedures for periodic testing and revision of contingency plans.		**PARTIAL** - Appendix L of the SSAA is to contain the Contingency Plans. Testing and Revision Procedures are normally part of a DoD Contingency Plan. This meets the requirement to document the plans as required under § 164.316, policies and procedures documentation. **PARTIAL** - C5.3.8. States that task 3-7 is "Contingency Plan Evaluation." The task description in subsection C5.3.8.2 states, "The contingency plan evaluation task analyzes the contingency, backup, and continuity of service plans to ensure the plans are consistent with the requirements identified in the SSAA. Periodic testing of the contingency plan is required by DoD Directive 5200.28 (reference (b)) for critical systems and is encouraged for all systems." The task description requires periodic testing for critical systems only instead of all systems and does not require revision of the plan based on the results of the testing.	DoD 5200.40-I DoD 8500.2-I MHS IA Policy/Guidance Manual (Feb 2003)
164.308(a)(7)(ii)(E)	Applications and Data Criticality Analysis: Assess the relative criticality of specific applications and data in support of other contingency plan components.		**MEETS** - Sections C3.4.2.2.3.2 and C3.4.2.2.3.3 require the SSAA to "define the system criticality and the acceptable risk[1] for the system in meeting the mission responsibilities" and "the type and sensitivity of the data processed by the system." It requires that the information be recorded in sections 1.3.2 and 1.3.3 of the SSAA.	DoD 8500.1-D DoD 8500.2-I
164.308(a)(8)	**Evaluation: Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.**	**Ref §3544(b)(6)** "a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency." **Ref §3545(a)(1)** "Each year each agency shall have performed an independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices."	**MEETS** - Section C1.3 DITSCAP Objective states "establishes a standard process, set of activities, general tasks, and a management structure to certify and accredit IS that will maintain the information assurance (IA) and security posture of the Defense Information Infrastructure (DII). … For a system in development, the intent is to identify appropriate security requirements, design to meet those requirements, test the design against the same requirements, and then monitor the accredited system for changes or reaccreditation as necessary." Maps almost completely. Unfortunately the last line concerning identifying appropriate security requirements refers only to developing systems even though it is true of all systems undergoing certification/accreditation. However, section C3.4.5.2.1 requires the CA team to identify and document "the security instructions or directives applicable to the system. In most cases, this will include **national level directives**, OMB Circulars A-123 and A-130, and DoD directives." Once the final rules are published the security and privacy standards would be among the national level directives that would be identified as requirements to be met by health related systems and networks. It does/would not refer to HIPAA by name however. This meets the requirement. The certification statements are contained in appendix R.	DoD 5000.2-R DoD 5200.40-I DoD 8500.1-D DoD 8500.2-I DoD 8510.1-M Policy/Guidance Manual (Feb 2003)

[1] While each Service or Agency has created their own definition of acceptable risk, the generally accepted use of the term is the "Judicious and carefully considered assessment by the DAA that the residual risk inherent in the operation of the IS or network is acceptable."

SECTION OF HIPAA SECURITY RULE	HIPAA SAFEGUARD	RELEVANT FISMA PROVISIONS	RELEVANT DITSCAP PROVISIONS As stated in the P3WG[1] relevant to DoD 8510.1-M	DoD Relevant References
164.308(b)(1)	**Business Associate Contracts and Other Arrangements: A covered entity, in accordance with Sec. 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only of the covered entity obtains satisfactory assurances, in accordance with Sec. 164.314(a) that the business associate appropriately safeguard the information.**	**Ref §3544(a)(1)(A)(ii)** states that the head of each agency shall be responsible for "...information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency"	**NONE**	DoD 6025.18-R DoD 8500.1-D DoD 8500.2-I MHS IA Policy/Guidance Manual (Feb 2003)
164.308(b)(4)	Written Contract or Other Arrangement: Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of Sec. 164.314(a).		**NONE**	DoD 6025.18-R DoD 8500.2-I MHS IA Policy/Guidance Manual (Feb 2003)
PHYSICAL SAFEGUARDS				
164.310(a)(1)	**Facility Access Controls: Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.**	**Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate" AND **Ref §3544(b)(8)** "plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency."	**MEETS** - Section C3.4.4.2.1 requires the SSAA to "describe the physical, personnel, communications, emanations, hardware, software, and procedural security features that will be necessary to support site operations. Operating environment security involves the measures designed to prevent unauthorized personnel from gaining physical access to equipment, facilities, material and documents and to safeguard the assets against espionage, sabotage, damage, and theft." Subsection C3.4.4.2.1.2 requires the SSAA to "identify the procedures needed to counter potential threats that may come from inside or outside the organization. Identify the routine office security practices that ensure unauthorized access to protected resources is prohibited." This is recorded in sections 2.1 and 2.1.2 of the SSAA. This requirement is met.	DoD 5200.8-R DoD 8500.2-I MHS IA Policy/Guidance Manual (Feb 2003)

SECTION OF HIPAA SECURITY RULE	HIPAA SAFEGUARD	RELEVANT FISMA PROVISIONS	RELEVANT DITSCAP PROVISIONS As stated in the P3WG[1] relevant to DoD 8510.1-M	DoD Relevant References
164.310(a)(2)(i)	Contingency Operations: Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	**Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate." **Ref §3544(b)(8)** "plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency."	**PARTIAL** - Appendix L of the SSAA is to contain the Contingency Plans. This meets the requirement to document the policies and procedures as required under § 164.316, policies and procedures documentation.	DoD 5200.8-R DoD 8500.2-I
164.310(a)(2)(ii)	Facility Security Plan: Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	**Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate." **Ref §3544(b)(8)** "plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency."	**MEETS** – C3.4.4.2.1.1, C3.4.4.2.1.2. Section C3.4.4.2.1.1 requires the SSAA to "describe the physical environment in which the system will operate including floor plans, equipment placement, electrical and plumbing outlets, telephone outlets, air conditioning vents, sprinkler systems, fences, and extension of walls from true floor to true ceiling." Section C3.4.4.2.1.2 requires the SSAA to "identify the procedures needed to counter potential threats that may come from inside or outside the organization and identify the routine office security practices that ensure unauthorized access to protected resources is prohibited." The policies and procedures that satisfy 10.2A would be documented in sections 2.1, 2.1.1, and 2.1.2.	DoD 5200.8-D DoD 5200.8-R DoD 8500.2-I MHS IA Policy/Guidance Manual (Feb 2003)

SECTION OF HIPAA SECURITY RULE	HIPAA SAFEGUARD	RELEVANT FISMA PROVISIONS	RELEVANT DITSCAP PROVISIONS As stated in the P3WG[1] relevant to DoD 8510.1-M	DoD Relevant References
164.310(a)(2)(iii)	Access Control and Validation Procedures: Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	**Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate." **Ref §3544(b)(8)** "plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency."	**PARTIAL** - Subsection C3.4.4.2.1.3 under Operating Environment requires the SSAA to "identify the administrative security procedures including the manual operations that counter threats." The policy/procedures requiring the "need-to-know procedures" would be documented in section 2.1.3 as required under §164.316, policies and procedures documentation, but it does not actually specify a requirement for "need-to-know procedures". **PARTIAL** - Section C3.4.4.2.1.2 requires the SSAA to identify the procedures needed to counter potential threats that may come from inside or outside the organization and identify the routine office security practices that ensure unauthorized access to protected resources is prohibited. The policies and procedures would be documented in section 2.1.2 as required under §164.316, policies and procedures documentation. This manual does not specifically state the types of procedures and practices required, just that they should be documented in this appendix." **PARTIAL** - Subsection C3.4.4.2.1.3 under Operating Environment requires the SSAA to "identify the administrative security procedures including the manual operations that counter threats." The procedures requiring the sign-in for visitors and escorts would be documented in section 2.1.3 as required under §164.316, policies and procedures documentation, but it does not actually specify a requirement for sign in logs or escorts for visitors. **PARTIAL** - C3.4.4.2.1.3, C3.4.4.2.2. Subsection C3.4.4.2.1.3 under Operating Environment requires the SSAA to "identify the administrative security procedures including the manual operations that counter threats." Section C3.4.4.2.2 requires the SSAA to "describe the system development approach and the environment within which the system will be developed. The system development approach is an information security strategy that incorporates security into each phase of a system's life cycle." Restriction of program testing and revision in the operational environment would be recorded in section 2.1.3 and in the development environment in section 2.2 as required under §164.316, policies and procedures documentation, but they do not actually specify a requirement for restriction of program testing and revision.	DoD 5200.8-R DoD 8500.2-I MHS IA Policy/Guidance Manual (Feb 2003)
164.310(a)(2)(iv)	Maintenance Records: Implement policies and procedures to document repairs and modifications to the physical components of a facility, which are related to security (for example, hardware, walls, doors, and locks).	**Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate" **Ref §3544(b)(8)** "plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency."	**PARTIAL** - Subsection C3.4.4.2.1.3 under Operating Environment requires the SSAA to "identify the administrative security procedures including the manual operations that counter threats." The procedures requiring the maintenance records would be documented in section 2.1.3 as required under § 164.316, policies and procedures documentation, but it does not actually specify a requirement for maintenance records.	DoD 8500.2-I

SECTION OF HIPAA SECURITY RULE	HIPAA SAFEGUARD	RELEVANT FISMA PROVISIONS	RELEVANT DITSCAP PROVISIONS As stated in the P3WG[1] relevant to DoD 8510.1-M	DoD Relevant References
164.310(b)	**Workstation Use: Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.**	**Ref §3544(a)(1)(A)** "providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—(i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." **Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate."	**PARTIAL** - Appendix J is to contain the "System Rules of Behavior" which would include workstation use. This meets the requirement to document the Policy/Guidance as required under § 164.316, policies and procedures documentation, but does not specifically mention workstations.	DoD 8500.2-I
164.310(c)	**Workstation Security: Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.**	**Ref §3544(a)(1)(A)** "providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—(i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." **Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate."	**MEETS** - Section C3.4.4.2.1.2 requires the SSAA to "identify the procedures needed to counter potential threat that may come from inside or outside the organization. Identify the routine office practices that ensure unauthorized access to protected resources is prohibited." While this does not specify workstations, they would fall under the definition of protected resources. These procedures would be documented in section 2.1.2.	DoD 8500.2-I

SECTION OF HIPAA SECURITY RULE	HIPAA SAFEGUARD	RELEVANT FISMA PROVISIONS	RELEVANT DITSCAP PROVISIONS As stated in the P3WG[1] relevant to DoD 8510.1-M	DoD Relevant References
164.310(d)(1)	**Device and Media Controls: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.**	**Ref §3544(a)(1)(A)** "providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—(i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." **Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate."	**PARTIAL** - C3.4.4.2.1 requires the section 2.1 of the SSAA to describe the operating environment security including "the measures designed to prevent unauthorized personnel from gaining physical access to equipment, facilities, material and documents and to safeguard the assets against espionage, sabotage, damage, and theft." This provision requires documentation of physical access controls as required under § 164.316, policies and procedures documentation, but does not specify what they should be.	DoD 8500.2-I MHS IA Policy/Guidance Manual (Feb 2003)
164.310(d)(2)(i)	Disposal: Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.		**NONE**	DoD 8500.2-I MHS IA Policy/Guidance Manual (Feb 2003)
164.310(d)(2)(ii)	Media Re-Use: Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.		**NONE**	DoD 8500.2-I
164.310(d)(2)(iii)	Accountability: Maintain a record of the movements of hardware and electronic media and any person responsible therefore.		**PARTIAL** - C3.4.4.2.1 requires the SSAA to describe the operating environment security including "the measures designed to prevent unauthorized personnel from gaining physical access to equipment, facilities, material and documents and to safeguard the assets against espionage, sabotage, damage, and theft." This language only refers to unauthorized access so may or may not include measures to record the actions of all users (including authorized users) with regard to electronic devices and media. This meets the requirement to document the implemented measures in section 2.1 as required under § 164.316, policies and procedures documentation, but does not specifically require accountability (logging related to media).	DoD 8500.2-I

SECTION OF HIPAA SECURITY RULE	HIPAA SAFEGUARD	RELEVANT FISMA PROVISIONS	RELEVANT DITSCAP PROVISIONS As stated in the P3WG[1] relevant to DoD 8510.1-M	DoD Relevant References
164.310(d)(2)(iv)	Data Backup and Storage: Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.		**NONE**	DoD 8500.2-I MHS IA Policy/Guidance Manual (Feb 2003)
TECHNICAL SAFEGUARDS				
164.312(a)(1)	**Access Controls: Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in Sec. 164.308(a)(4)..**	**Ref §3544(a)(1)(A)** "providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—(i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." **Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate."	**PARTIAL -** C3.4.5.2.4, C3.4.6.2. Section C3.4.5.2.4 requires section 4.4 of the SSAA to "describe the security CONOPS (Concept of Operations) including system input, system processing, final outputs, security controls and interactions and connections with external systems." The technical access control methods would be included as security controls in a CONOPS. Appendix D contains the System CONOPS. C3.4.6.2 states the system architecture task "defines the system hardware, software, firmware, and interfaces. This description contains an overview of the internal system structure including the anticipated hardware configuration, application software, software routines, operating systems, remote devices, communication processors, network, and remote interfaces." Input to this task includes the Architecture and Design documents, which will document technical security controls. These documents would be included in appendix I. This meets the requirement to document access control as required under § 164.316, policies and procedures documentation, but does not specifically require technical access control.	DoD 8500.1-D DoD 8500.2-I MHS IA Policy/Guidance Manual (Feb 2003)

SECTION OF HIPAA SECURITY RULE	HIPAA SAFEGUARD	RELEVANT FISMA PROVISIONS	RELEVANT DITSCAP PROVISIONS As stated in the P3WG[1] relevant to DoD 8510.1-M	DoD Relevant References
164.312(a)(2)(i)	Unique User Identification: Assign a unique name and/or number for identifying and tracking user identity.		**PARTIAL** - C3.4.5.2.4, C3.4.6.2. Section C3.4.5.2.4 requires section 4.4 of the SSAA to "describe the security CONOPS (Concept of Operations) including system input, system processing, final outputs, security controls and interactions and connections with external systems." Unique user identification would be included as a security control in a CONOPS. C3.4.6.2 states the system architecture task "defines the system hardware, software, firmware, and interfaces. This description contains an overview of the internal system structure including the anticipated hardware configuration, application software, software routines, operating systems, remote devices, communication processors, network, and remote interfaces." Input to this task includes the Architecture and Design documents, which will document technical security controls. These documents would be included in appendix I. This meets the requirement to document the use of unique user identification as required under § 164.316, policies and procedures documentation, but does not specifically require it.	DoD 8500.2-I MHS IA Policy/Guidance Manual (Feb 2003)
164.312(a)(2)(ii)	Emergency Access Procedure: Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.		**PARTIAL** - C3.4.5.2.4 requires section 4.4 of the SSAA to "describe the security CONOPS (Concept of Operations) including system input, system processing, final outputs, security controls and interactions and connections with external systems." Appendix L is to contain the Contingency Plan. This meets the requirement to document the procedures for emergency access as required under § 164.316, policies and procedures documentation, but does not specify a requirement for the procedures.	
164.312(a)(2)(iii)	Automatic Logoff (Addressable): Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.		**PARTIAL -** C3.4.5.2.4, C.4.6.2. Section C3.4.5.2.4 requires section 4.4 of the SSAA to "describe the security CONOPS (Concept of Operations) including system input, system processing, final outputs, security controls and interactions and connections with external systems." Automatic logoff would be included as a security control in a CONOPS. C3.4.6.2 states the system architecture task "defines the system hardware, software, firmware, and interfaces. This description contains an overview of the internal system structure including the anticipated hardware configuration, application software, software routines, operating systems, remote devices, communication processors, network, and remote interfaces." Input to this task includes the Architecture and Design documents, which will document technical security controls. These documents would be found in appendix I. This meets the requirement to document the use of an automatic logoff as required under § 164.316, policies and procedures documentation, but does not specifically require it.	

SECTION OF HIPAA SECURITY RULE	HIPAA SAFEGUARD	RELEVANT FISMA PROVISIONS	RELEVANT DITSCAP PROVISIONS As stated in the P3WG[1] relevant to DoD 8510.1-M	DoD Relevant References
164.312(a)(2)(iv)	Encryption and Decryption (Addressable): Implement a mechanism to encrypt and decrypt electronic protected health information.		**PARTIAL** - C3.4.5.2.4, C3.4.6.2. Section C3.4.5.2.4 requires section 4.4 of the SSAA to "describe the security CONOPS (Concept of Operations) including system input, system processing, final outputs, security controls and interactions and connections with external systems." Encryption would be included as a security control in a CONOPS. C3.4.6.2 states the system architecture task "defines the system hardware, software, firmware, and interfaces. This description contains an overview of the internal system structure including the anticipated hardware configuration, application software, software routines, operating systems, remote devices, communication processors, network, and remote interfaces." Input to this task includes the Architecture and Design documents, which will document technical security controls. These documents would be found in appendix I. This meets the requirement to document the use of encryption as required under § 164.316, policies and procedures documentation, but does not specifically require it.	DoD 8500.2-I DoD 8510.1-M MHS IA Policy/Guidance Manual (Feb 2003)
164.312(b)	**Audit Controls: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.**	**Ref §3544(a)(1)(A)** "providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—(i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." **Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate."	**PARTIAL** - C3.4.5.2.4, C3.4.6.2. Section C3.4.5.2.4 requires section 4.4 of the SSAA to "describe the security CONOPS (Concept of Operations) including system input, system processing, final outputs, security controls and interactions and connections with external systems." Audit controls would be included as a security control in a CONOPS. C3.4.6.2 states the system architecture task "defines the system hardware, software, firmware, and interfaces. This description contains an overview of the internal system structure including the anticipated hardware configuration, application software, software routines, operating systems, remote devices, communication processors, network, and remote interfaces." Input to this task includes the Architecture and Design documents, which will document technical security controls. These documents would be found in appendix I. This meets the requirement to document the use of audit controls as required under § 164.316, policies and procedures documentation, but does not specifically require it.	DoD 8500.2-I DoD 8510.1-M MHS IA Policy/Guidance Manual (Feb 2003)

SECTION OF HIPAA SECURITY RULE	HIPAA SAFEGUARD	RELEVANT FISMA PROVISIONS	RELEVANT DITSCAP PROVISIONS As stated in the P3WG[1] relevant to DoD 8510.1-M	DoD Relevant References
164.312(c)(1)	**Integrity: Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.**	**Ref §3544(a)(1)(A)** "providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—(i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." **Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate."	**PARTIAL** - C3.4.5.2.4, C3.4.6.2. Section C3.4.5.2.4 requires section 4.4 of the SSAA to "describe the security CONOPS (Concept of Operations) including system input, system processing, final outputs, security controls and interactions and connections with external systems." Data authentication would be included as a security control in a CONOPS. C3.4.6.2 states the system architecture task "defines the system hardware, software, firmware, and interfaces. This description contains an overview of the internal system structure including the anticipated hardware configuration, application software, software routines, operating systems, remote devices, communication processors, network, and remote interfaces." Input to this task includes the Architecture and Design documents, which will document technical security controls. These documents would be found in appendix I. This meets the requirement to document the use of policies and procedures to ensure data integrity as required under § 164.316, policies and procedures documentation, but does not specifically require it.	DoD 8500.2-I DoD 8510.1-M MHS IA Policy/Guidance Manual (Feb 2003)
164.312(c)(2)	Mechanism to Authenticate Electronic Protected Health Information: Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.		**PARTIAL** - C3.4.5.2.4, C3.4.6.2. Section C3.4.5.2.4 requires section 4.4 of the SSAA to "describe the security CONOPS including system input, system processing, final outputs, security controls and interactions and connections with external systems." Data authentication would be included as a security control in a CONOPS. C3.4.6.2 states the system architecture task "defines the system hardware, software, firmware, and interfaces. This description contains an overview of the internal system structure including the anticipated hardware configuration, application software, software routines, operating systems, remote devices, communication processors, network, and remote interfaces." Input to this task includes the Architecture and Design documents, which will document technical security controls. These documents would be found in appendix I. This meets the requirement to document the use of mechanism to authenticate data as required under § 164.316, policies and procedures documentation, but does not specifically require it.	DoD 8500.2-I DoD 8510.1-M MHS IA Policy/Guidance Manual (Feb 2003)

SECTION OF HIPAA SECURITY RULE	HIPAA SAFEGUARD	RELEVANT FISMA PROVISIONS	RELEVANT DITSCAP PROVISIONS As stated in the P3WG[1] relevant to DoD 8510.1-M	DoD Relevant References
164.312(d)	**Person or Entity Authentication: Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.**	**Ref §3544(a)(1)(A)** "providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—(i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." **Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate."	**PARTIAL** - C3.4.5.2.4, C3.4.6.2. Section C3.4.5.2.4 requires section 4.4 of the SSAA to "describe the security CONOPS (Concept of Operations) including system input, system processing, final outputs, security controls and interactions and connections with external systems." Entity authentication would be included as a security control in a CONOPS. C3.4.6.2 states the system architecture task "defines the system hardware, software, firmware, and interfaces. This description contains an overview of the internal system structure including the anticipated hardware configuration, application software, software routines, operating systems, remote devices, communication processors, network, and remote interfaces." Input to this task includes the Architecture and Design documents, which will document technical security controls. These documents would be found in appendix I. This meets the requirement to document the use of entity authentication as required under § 164.316, policies and procedures documentation, but does not specifically require it.	DoD 8500.1-D DoD 8500.2-I DoD 8510.1-M MHS IA Policy/Guidance Manual (Feb 2003)
164.312(e)(1)	Transmission Security: Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	**Ref §3544(a)(1)(A)** "providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—(i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." **Ref §3544(b)(3)** "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate."	**PARTIAL** – C3.4.6.2.4 requires the SSAA to "describe the system's external interfaces including the purpose of each external interface and the relationship between the interface and the system. Describe the significant features of the communications layout, including a high level diagram of the communications links and encryption techniques connecting the components of the system, associated data communication, and networks." This meets the requirement to document the technical security mechanisms in section 3.2 of the SSAA as required under § 164.316, policies and procedures documentation, but does not specifically require that they exist.	DoD 8500.1-D DoD 8500.2-I DoD 8510.1-M MHS IA Policy/Guidance Manual (Feb 2003)
164.312(e)(2)(i)	Integrity Controls: Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.		**PARTIAL** - C3.4.6.2.4 requires the SSAA to "describe the system's external interfaces including the purpose of each external interface and the relationship between the interface and the system. Describe the significant features of the communications layout, including a high level diagram of the communications links and encryption techniques connecting the components of the system, associated data communication, and networks." This meets the requirement to document the integrity controls in section 3.2 of the SSAA as required under §164.316, policies and procedures documentation, but does not specifically require that they exist.	DoD 8500.1-D DoD 8500.2-I DoD 8510.1-M MHS IA Policy/Guidance Manual (Feb 2003)

SECTION OF HIPAA SECURITY RULE	HIPAA SAFEGUARD	RELEVANT FISMA PROVISIONS	RELEVANT DITSCAP PROVISIONS As stated in the P3WG[1] relevant to DoD 8510.1-M	DoD Relevant References
164.312(e)(2)(ii)	Encryption (Addressable): Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.		**PARTIAL** – C3.4.6.2.4 requires the SSAA to "describe the system's external interfaces including the purpose of each external interface and the relationship between the interface and the system. Describe the significant features of the communications layout, including a high level diagram of the communications links and encryption techniques connecting the components of the system, associated data communication, and networks." This meets the requirement to document the encryption in section 3.2 of the SSAA as required under § 164.316, policies and procedures documentation, but does not specifically require it.	DoD 8500.2-I DoD 8510.1-M MHS IA Policy/Guidance Manual (Feb 2003)

1 – Location of the P3WG Report: https://rimr.tatrc.org under References/Reports/HIPAA Security